ICION 6TH CONFERENCE 2018

Why Your Security System Still Failed on Facing Today Cyber Crime

SEEING WHAT OTHERS DON'T

Henry Kristianto

Enterprise Sales Director

Fireeye

06th March 2018, Ambarrukmo Yogyakarta

ROYAL AMBARRUKMO
YOGYAKARTA

ICION
Indonesian CIO Network

THE WORST CASE SCENARIO

2

Saudi Aramco – Biggest $$ hack in history (Oil&Gas)

Saudi Aramco suffered the worst hack in world history in 2012.

Aug 15, 2012 (Ramadan)

Aramco was hit by malware Shamoon, rendered 35000 computers partially wiped or totally destroyed – used typewriters and faxes for few weeks

Successful spear phishing attack by group “Cutting Sword of Justice” .
Aramco’s ww operations were unplugged from internet to stop the spread of Shamoon.
Aramco took 5 months to recover

http://www.darkreading.com/attacks-breaches/inside-the-aftermath-of-the-saudi-aramco-breach/d/d-id/1321676

Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid
https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

4

$81M Bangladesh Bank Heist…

Feb 4, 2016

Attacker use stolen SWIFT credentials of Bangladesh Central Bank to send more than three dozen fraudulent money transfer requests to the Federal Reserve Bank of New York asking the bank to transfer millions of the Bangladesh Bank's funds to bank accounts in the Philippines & Sri Lanka.

After the Bangladesh Bank Heist …..Not an isolated incident

CNBC

Search Quotes, News & Video

HOME U.S. NEWS MARKETS INVESTING TECH MAKE IT VIDEO SHOWS PRIMETIME MORE

CYBERSECURITY

TECHNOLOGY | RE/CODE | MOBILE | SOCIAL MEDIA | ENTERPRISE | GAMING | CYBERS

Vietnam's Tien Phong Bank says it was second bank hit by SWIFT cyberattack

Sunday, 15 May 2016 | 7:52 PM ET

REUTERS

Nguyen Huy Kham

A man rides a motorcycle past the Vietnamese commercial Tien Phong bank in Hanoi May 13, 2016.

May 15, 2016

Hanoi-based TPBank said in a statement late on Sunday in response to inquiries from Reuters that in the fourth quarter of last year it identified suspicious requests through fraudulent SWIFT messages to transfer more than 1 million euros ($1.1 million) of funds.

6

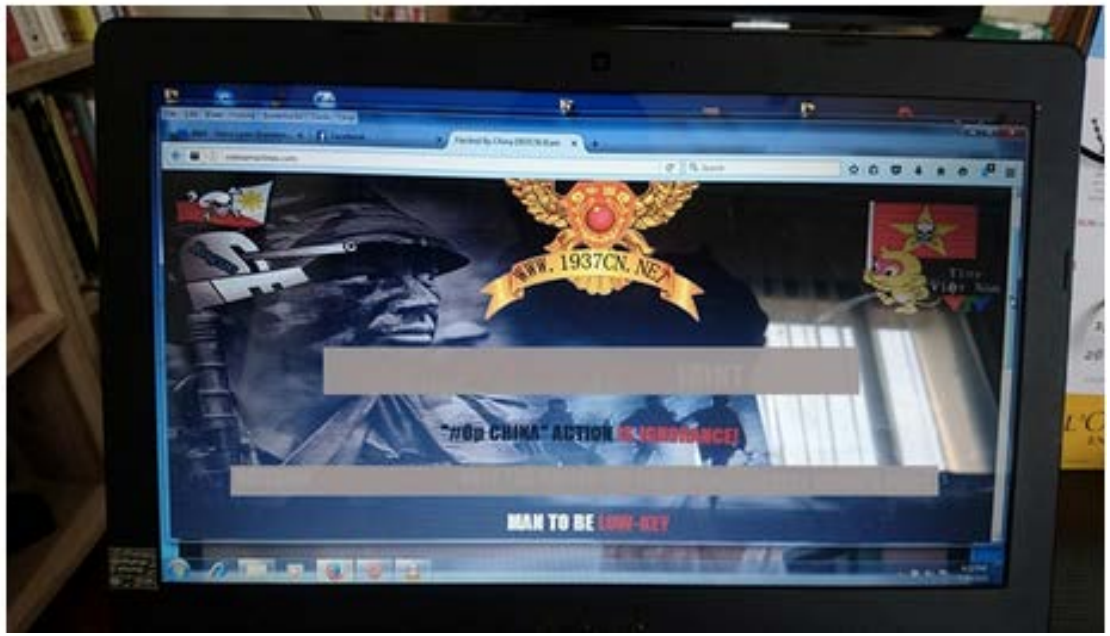
Source: http://www.cnbc.com/2016/05/15/vietnams-tien-phong-bank-says-it-was-second-bank-hit-by-swift-cyber-attack.html

FireEye

Vietnam Airports Cyber Attacks well planned & targetted

Chinese hackers attack VN's airports and Vietnam Airlines' website

Update: July, 29/2016 - 09:00



July 29, 2016

The hackers used a brand new type of malware able to pass normal security tools, such as antivirus software," VNISA said.

In the case of Vietnam Airlines, VNISA said there are signs showing that hackers may have penetrated the airline's system as early as mid-2014.

http://tuoitrenews.vn/society/36289/cyber-attacks-on-vietnam-airports-are-wellplanned-association

ROYAL AMBARRUKMO
YOGYAKARTA

FireEye with Front Line Experience

FireEye

HEADLINE :

Target settles with banks for $39 million after epic data breach

BREACHED :

2013

VICTIM :

IMPACT:

- Estimated $300M of total impact
- CEO resignation
- CIO resignation
- 40 million customers effected

RESPONDER :

FireEye

FireEye

HEADLINE :

Sony Got Hacked Hard: What We Know and Don’t Know So Far

BREACHED :

2014

RESPONDER :

FireEye

VICTIM :

IMPACT:

- Leaked emails between Sony Pictures executives
- Sony Pictures Co-chairman resignation
- $15M USD in Incident Response and Remediation Costs
- Computer Networks shut down for several weeks

FireEye

HEADLINE :

Hacked Toymaker VTech Admits Breach Actually Hit 6.3 Million Children

BREACHED :

2015

VICTIM :

vtech

IMPACT:

- 6.3 Million Parents & Children affected when thousands of pictures, as well as a year's worth of chat logs, were compromised

RESPONDER :

FireEye

FireEye

HEADLINE :

Anthem, a Major Health Insurer, Suffered a Massive Hack

BREACHED :

2015

VICTIM :

Anthem®

IMPACT:

- Personal Information of 80 Million Customers Stolen

RESPONDER :

FireEye

HEADLINE :

Verizon Demands a Better Deal After Yahoo's Latest Historic Hack

BREACHED :

2016

VICTIM :

YAHOO!

IMPACT:

- 1 Billion User Accounts were hacked
- $4.8B acquisition deals by Verizon impacted
- 2nd time criminal charges are filed against known state actors for hacking

RESPONDER :

FireEye

FireEye

HEADLINE :

Bangladesh Bank Chief Resigns After Cyber Theft of $81 Million

BREACHED :

2016

VICTIM :

IMPACT:

- $81 Million Dollar Theft
- Resignation of Central Bank's Governor

RESPONDER :

FireEye

HEADLINE :

Food Court: Arby's Reportedly Faces 8 Lawsuits Resulting from Breach

BREACHED :

2017

VICTIM :

IMPACT:

- Over 350,000 credit and debit card accounts may have been impacted by the hack, according to the credit union service PSCU

RESPONDER :

FireEye

FireEye

HEADLINE :

Sabre Discloses Data Breach of Card Details at its Hotels

BREACHED :

2017

VICTIM :

Sabre

IMPACT:

- Significant breach of payment and customer data tied to bookings processed through a reservations system that serves more than 32,000 hotels and other lodging establishments

RESPONDER :

FireEye

FireEye

HEADLINE :

Equifax negligence causes loss of customer data

BREACHED :

2017

VICTIM :

IMPACT:

- Breach resulted in loss of customer data, which now “permits thieves to create FAKE identities, fraudulently obtain loans, swipe tax refunds and destroy” consumer creditworthiness.

RESPONDER :

FireEye

FireEye

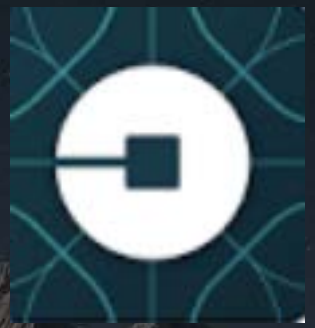
HEADLINE :

Uber paid 100K to hackers to delete data and keep quiet about breach

BREACHED :

2017

VICTIM :



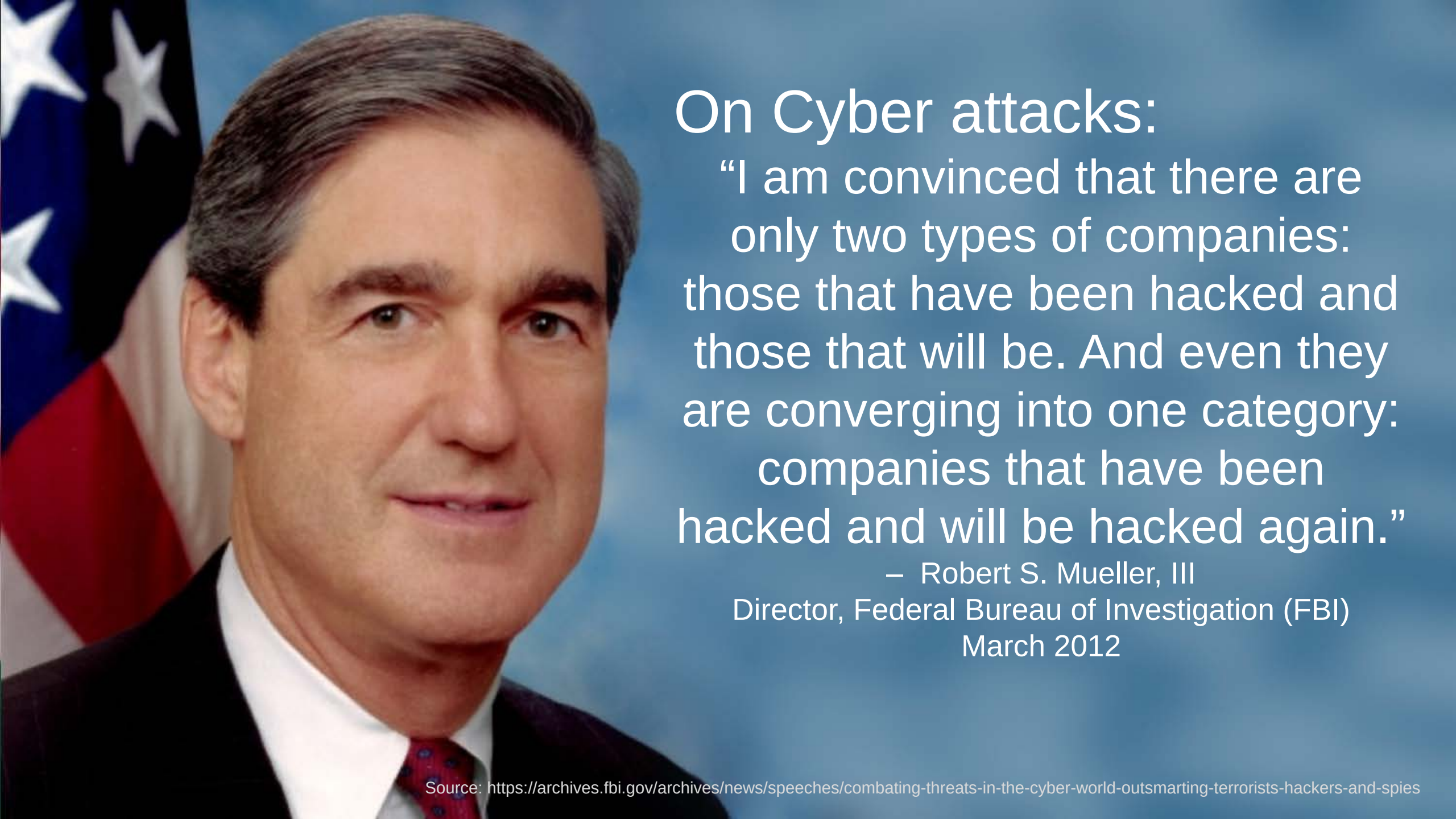
IMPACT:

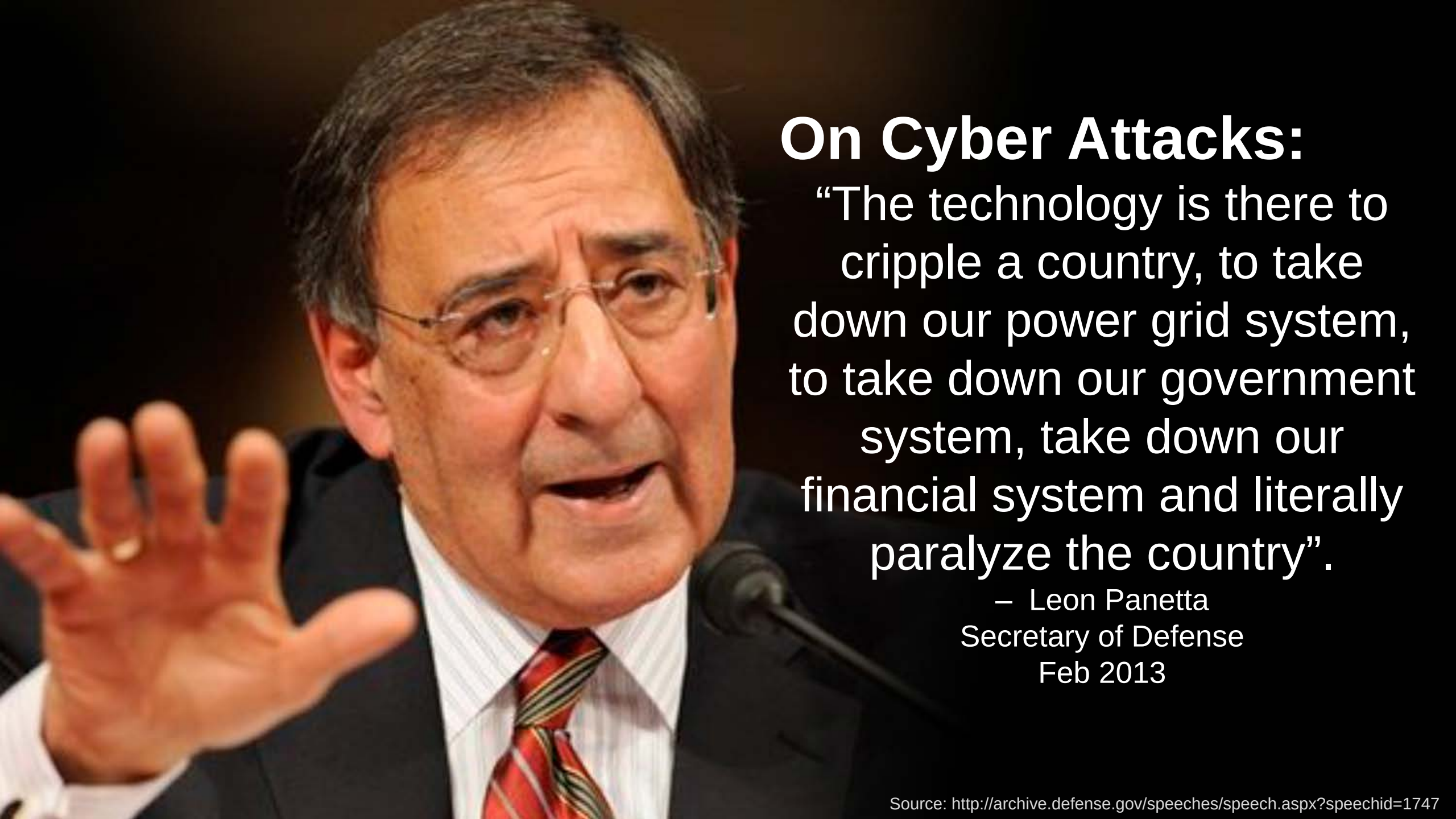
- Personal Information of 57M customers and drivers data compromised, deleted and now disclosed to Public after more than 1 Year

RESPONDER :

FireEye

LEADER PERSPECTIVE : SERIOUSNESS OF CYBER RISK


On Cyber attacks:
“I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.”
– Robert S. Mueller, III
Director, Federal Bureau of Investigation (FBI)
March 2012
Source: https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies

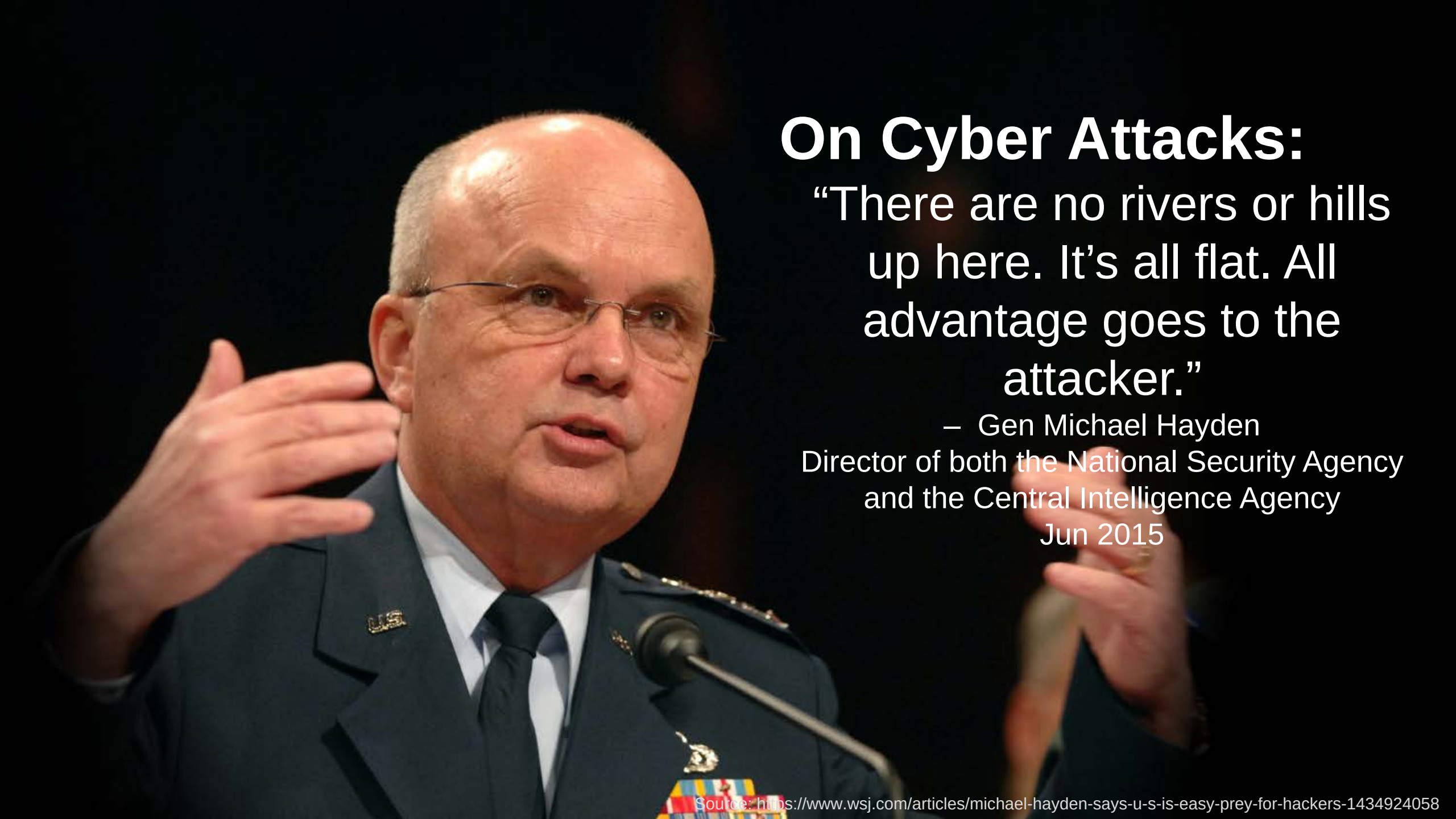


On Cyber Attacks:

"The technology is there to cripple a country, to take down our power grid system, to take down our government system, take down our financial system and literally paralyze the country".

– Leon Panetta
Secretary of Defense
Feb 2013

Source: http://archive.defense.gov/speeches/speech.aspx?speechid=1747



On Cyber Attacks:

"There are no rivers or hills up here. It's all flat. All advantage goes to the attacker."

– Gen Michael Hayden
Director of both the National Security Agency and the Central Intelligence Agency
Jun 2015

Source: https://www.wsj.com/articles/michael-hayden-says-u-s-is-easy-prey-for-hackers-1434924058

CORRECTING COMMON MISCONCEPTIONS


Breaches Are Inevitable
Technology Alone Will Not Save You
Your Data Is More Important Than You Think


Achievable Security Objective:
No Business Impact Resulting
From Cyber Attack

3 Truths in Cyber-security

- Organizations don’t have enough security people
- Most organizations get too many alerts
- Eventually bad guys get in, and most organizations are not aware

“Alert to fix in minutes, from an iPAD, sitting in a Starbucks café in the airport”

- Kevin Mandia, FireEye CEO

Traditional “Defense in Depth” is failing

The New Breed of Attacks Evade Signature-Based Defenses

APT* is a “WHO”….. Not a “WHAT”

* APT : Advanced Persistent Threat

Malware

Attacker

Define your goal carefully

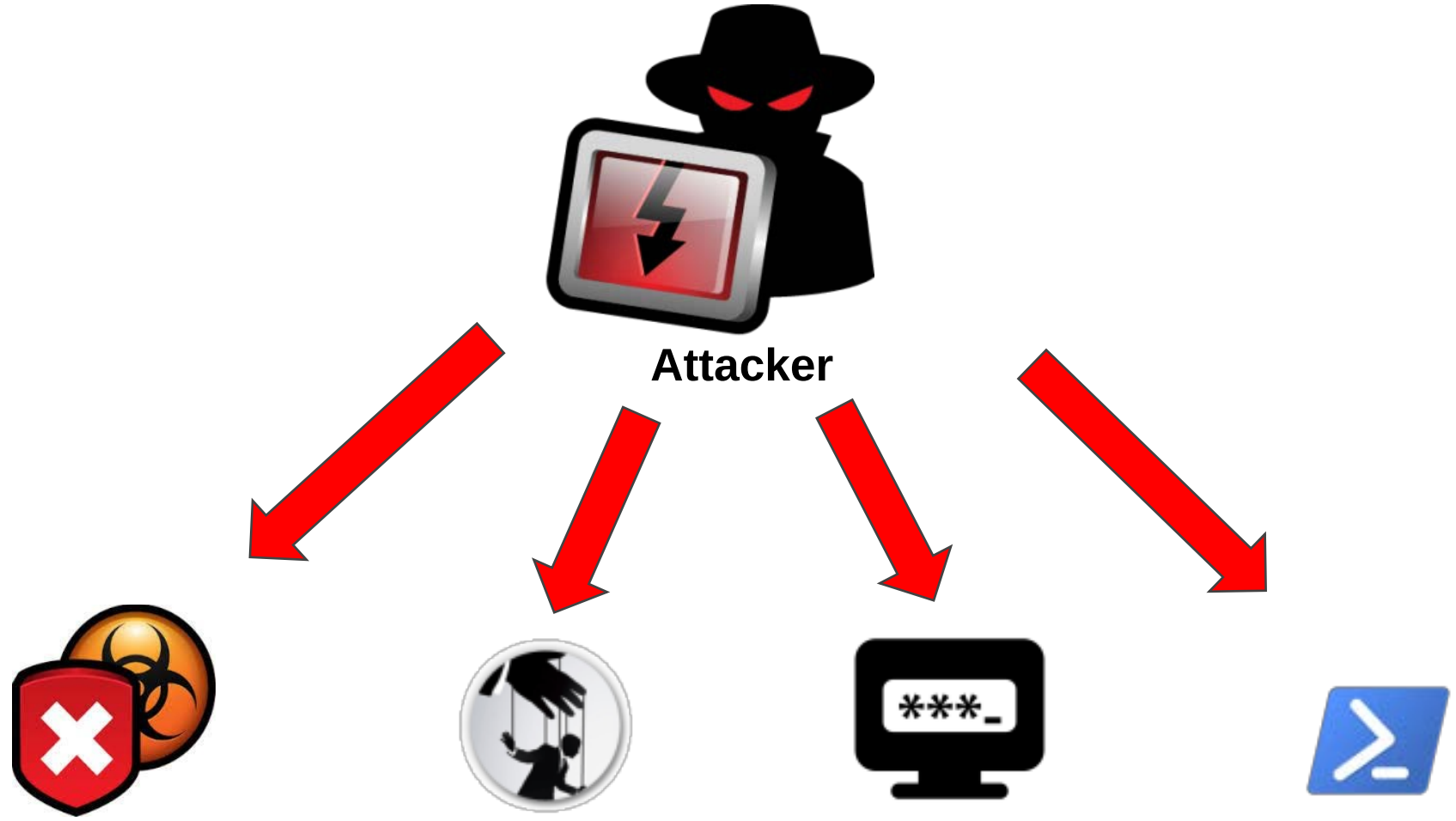
Are you trying to solve the

APT problem

by catching more malware?

FireEye

Malware is just one of the attacker’s many tools



Attack Lifecycle

Maintain Presence

Lateral Movement

Initial Recon

Initial Compromise

Establish Foothold

Escalate Privileges

Internal Recon

Complete Mission

DWELL TIME / IMPACT : 520 days

Identify Exploitable Vulnerabilities

Gain Initial Access Into Target

Strengthen Position within Target

Steal Valid User Credentials

Identify Target Data

Package and Steal Target Data

PREVENTION

RESPONSE

DETECTION

Malware Problem

Human Attacker Problem

Endpoint EPP

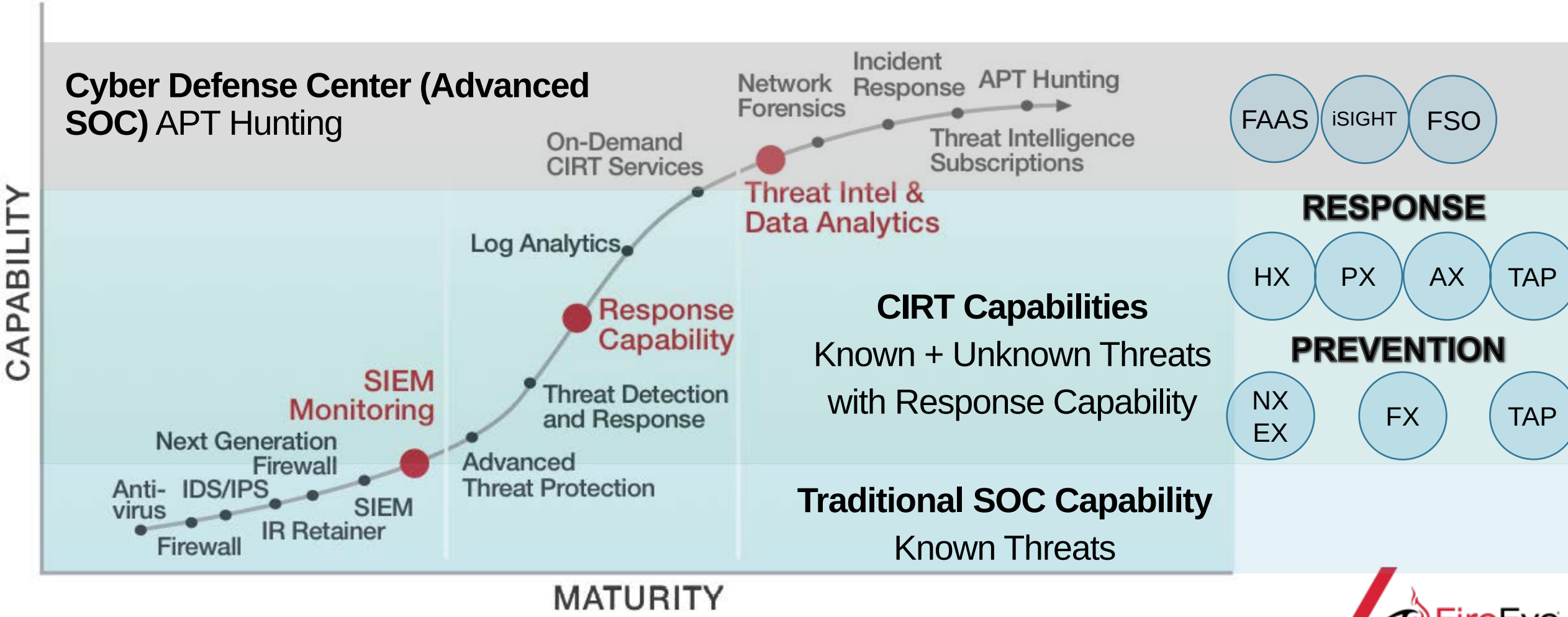
Endpoint Detection and Response (EDR)

FireEye + Partners

BREACH

FireEye

Next Step : Cyber Program Maturity



Sample Forensic Data : Malware CallBack (High Critical Severity)

Malware : Trojan.Ponmocup

Attacker CnC

Page: 1 of 1

	Type	Id	FT	Malware	Severity	Time (WIB)	Source IP	Target IP	URL / Md5sum	Location	SC Version	Badges
▼	Malware Callback	5539		Trojan.Ponmocup	■■■■■■■	01/25/17 14:40:35	192.168.18.212	149.244.34.119	http://149.244.34.119/info/go.php	DE	570.174	Blocked

Callback: ■ Trojan.Ponmocup

Interface: network A (mode inline, port A2)

Blocking Action: Blocked

Set Sig Name Blocking Policy: None ▼ for **Trojan.Ponmocup**

Set Sig ID Blocking Policy: None ▼ for **20005160**

Communication Capture: pcap 1119 bytes (text)

Raw Alert: Download (xml)

IP Protocol: TCP

Victim IP: 192.168.18.212

Src MAC Address: f4:0f:1b:77:e6:45

Dst MAC Address: 08:5b:0e:ab:6b:2f

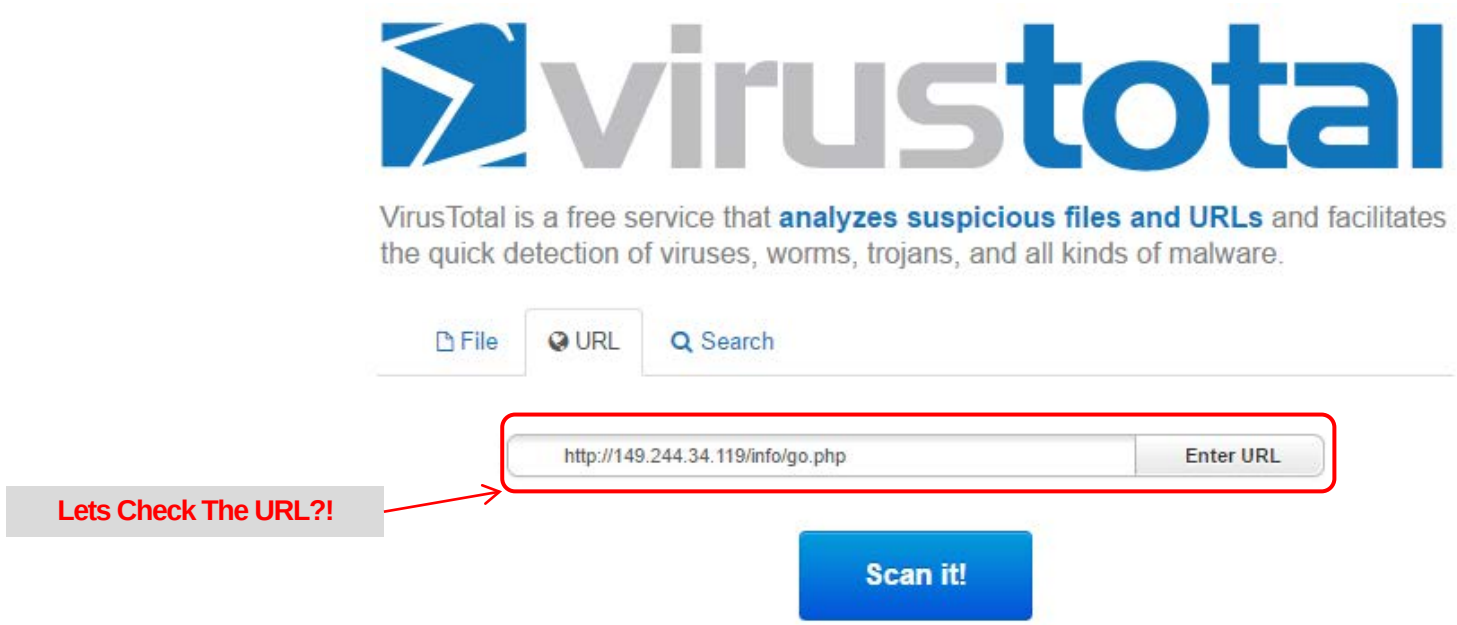
Callback communication from infected host:

Server DNS Name: *149.244.34.119* Service Port: *80* Location: *DE* Signature Name: *Trojan.Ponmocup*

Time Founded

Victim IP / HOST

Lets Check The URL?!



Lets Check The URL?!

FireEye

INCOMPLETE PLATFORMS = INCOMPLETE SOLUTIONS

Legacy Platforms

- Endpoint AV
- Endpoint Encryption
- Endpoint APT

“Next-Gen” Legacy Platforms

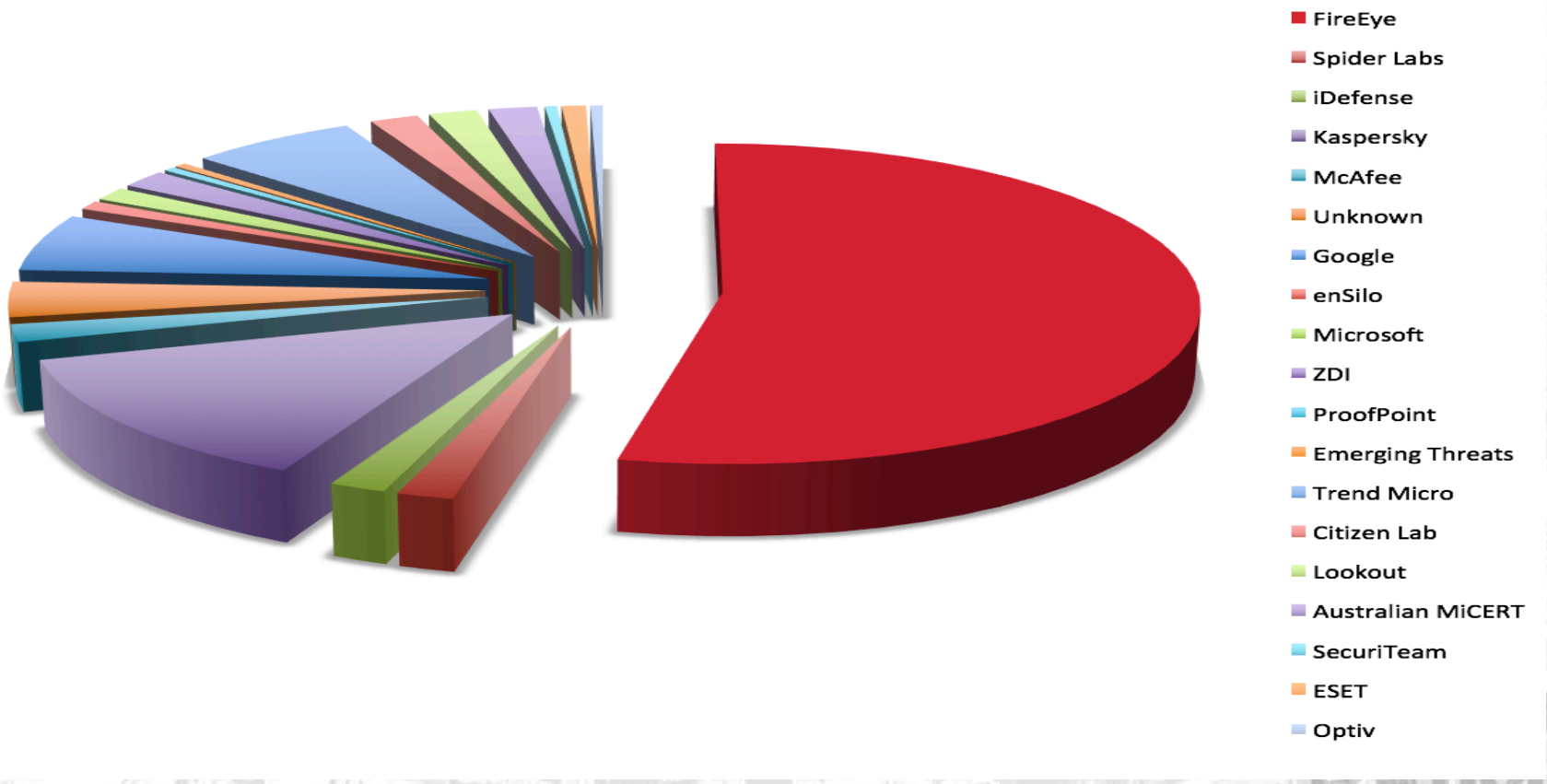
- Endpoint AV
- Endpoint Encryption
- Endpoint APT
- Visibility into Activity
- Exploit Detection & Prevention
- Endpoint Forensics, Alerts

FireEye Endpoint

- Endpoint AV
- Endpoint APT
- Visibility into Activity
- Exploit Detection & Prevention
- Endpoint Forensics, Alerts
- Integrated Workflow Platform
- Tactical/Operational Intel
- Incident Response / Assessment

The FireEye Difference : Seeing what others don't

The vital / key point measurement for Advanced Threat Detection vendor is a zero day detection track record. FireEye has an excellent zero day detection track record. As per September 2017, FireEye has found 30 from total of 56 zero-day attack (54%). This is much more than all the vendor detection to the zero day combined.



The FireEye Difference : Seeing what others don't

Zero Day Score Card

Updated on: 09-14-17

Vendors (2012-17)	Count	Percent
FireEye	30	54%
Spider Labs	1	2%
iDefense	1	2%
Kaspersky	7.5	13%
McAfee	1	2%
Unknown	2	4%
Google	3.25	6%
enSilo	0.5	1%
Microsoft	0.75	1%
ZDI	1	2%
ProofPoint	0.25	0%
Emerging Threats	0.25	0%
Trend Micro	3.5	6%
Citizen Lab	1	2%
Lookout	1	2%
Australian MiCERT	1	2%
SecuriTeam	0.25	0%
ESET	0.5	1%
Optiv	0.25	0%
Zero Day Totals	56	100%

Zero Day Summary (by Year)

2012	2013	2014	2015	2016	2017	Total
2	9	6	8	2.25	2.75	30.0
0	1	0	0	0	0	1
0	1	0	0	0	0	1
0	0	3	0.5	4	0	7.5
0	1	0	0	0	0	1
0	0	1	0	1	0	2
0	1	1	0	1.25	0	3.25
0	0	0	0.5	0	0	0.5
0	0	0	0.5	0	0.25	0.75
0	0	1	0	0	0	1
0	0	0	0	0.25	0	0.25
0	0	0	0	0.25	0	0.25
0	0	0	3.5	0	0	3.5
0	0	0	0	1	0	1
0	0	0	0	1	0	1
0	0	0	0	1	0	1
0	0	0	0	0	0.25	0.25
0	0	0	0	0	0.5	0.5
0	0	0	0	0	0.25	0.25
2	13	12	13	12	4	56.00

**Note: Shared 0-Day Discovery by 2 is recognized as .5, while 4 shared is .25 recognition*

Call to Vannie if need more info on Fireeye

+62 877 7567 8589

Email Vannie@advancedtechpac.com

SECURITY REIMAGINED

LARGE AND GROWING SET OF CUSTOMERS

GOVERNMENT

U.S. Department of Energy
FDIC
FBI
California Republic
U.S. Army
U.S. Air Force

INFRASTRUCTURE

SK telecom
GE
Northrop Grumman
Boeing
Airbus
Los Angeles World Airports
ConocoPhillips
Chevron
Verizon
Qualcomm
Lockheed Martin

HIGH TECH

Juniper Networks
Yahoo!
SAP
Mercado Libre
eBay
Twitter
facebook
zynga
Netflix
Adobe
Reuters
Samsung

HEALTHCARE

Genentech
A Member of the Roche Group
AMA
American Medical Association
UnitedHealthcare
Boston Scientific
Baxter
Sanofi
MD Anderson Cancer Network
BlueCross BlueShield
Medtronic
Kaiser Permanente

FINANCIAL SERVICES, INSURANCE

VISA
Wells Fargo
Capital One
BMO
Deloitte.
SallieMae
Deutsche Bank
Bank of England

RETAIL

Safeway
Nike
Marriott
NEC
ESPN
Bass Pro Shops
Nikon
LG Electronics
Chrysler

SMALL MEDIUM ENTERPRISE

electoral commission NSW
Alliant credit union
DARPA
EECS
Bush's Best
DATACOM
D-Wave The Quantum Computing Company
Draper Laboratory
rfmd Powered to Connect
Blackstone
Omnicell
Torys LLP
netpoleon Network · Security
Fandango
DVI
Sypris Solutions
Alston & Bird LLP
William Blair


ECONOMY IN INDONESIA
CIO NETWORK 6TH CONFERENCE
rrukmo Hotel Yogyakarta March 05th to 7th, 2018
www.icion-leadership.com
asg
rubrik
Labris
Bitdefender
WGS

FireEye


SHAPING AND SECURING
THE DIGITAL ECONOMY
IN INDONESIA
INDONESIAN CIO NETWORK 6TH CONFERENCE
05TH ,06TH AND 07TH OF MARCH 2018
Royal Ambarrukmo Yogyakarta
www.icion-leadership.com
Auddy +62 878 7724 6011
icion@advancedtechpac.com
Supporting Organizations:
ABDI
KOMINFO
(ISC)²
Key Media Partner:
KOMITe.id
ICT NEWS PORTAL & MAGAZINE

Henry Kristianto
Enterprise Sales Director

Henry Kristianto is an Innovative and self starter having over than 14 years of experience in Indonesia ICT industry.

He now runs FireEye Business in Indonesia, leading our business growth with enterprise customers in key sectors o Financial Services, Telecommunications and Government.

Henry's key strengths are in Sales and Marketing, Enterprise-Commercial Solutions & Market. Good with partners and customers, he is a strong leader and Cyber IT veteran who is able to open markets , build and drive Brand awareness and closure.

Thank You, see you in ICION 2019

- Support our effort to build a Safer Cyber Security World in Indonesia. Our official CISSP classes scheduled for April 23th to 27th 2018

- Contact to Vannie via +62 877 7567 8589
- Join us in our Linkedin Group ICION as below
- https://www.linkedin.com/groups/3942786

ICION
Indonesian CIO Network

See you in ICION 7th Conference, 2019 in Bali